DOI 10.29042/2018-3710-3715

Helix Vol. 8(5): 3710- 3715

What's Vulnerable in WhatsApp

[1]Sumitra Biswal, [2]Vishal Gupta
[1]Surya Consultants, Noida, India
[2] Jangoo Technologies, New Delhi, India
Email: sbiswal2912@gmail.com, vishal258120@gmail.com

Received: 09th July 2018, Accepted: 14th August 2018, Published: 31st August 2018

Abstract
The advent of Smartphones and their quick time services have made the urban lifestyle convenient and close-knit. Smartphone users can now reach their closed ones instantaneously via audio-video and messages. The Over-The-Top (OTT) applications have connected the users worldwide and bridged the gaps amidst scattered relations. While OTT applications have turned out to be blissful for dispersed relatives and have helped various commercial relations thrive, their security has never been well addressed. It is evident owing to multiple such applications emerging at a faster scale with Quality of Service (QoS) prioritized over security. The paper highlights certain major vulnerabilities and security flaws of the most popular OTT application, WhatsApp. This paper also acknowledges existing work pertaining to security of WhatsApp and similar web applications. In this paper we highlight an unaddressed vulnerability of WhatsApp that users are interestingly, not aware of. Besides, we also propose a novel method to ensure security of WhatsApp and akin applications against this silent-yet-deadly vulnerability discovered.

Keywords: WhatsApp, Mobile Applications, Authentication, Security, OTT, Web Applications

Introduction

The field of communication has evolved over time at a fast pace. The era of using Pigeons and Horses for communication has gradually been replaced by Postal means via roads, seas and airways. Sooner, the duration of transaction of messages was shortened with the Computer era. E-mails took over the industry thereby, reducing years and months to hours and minutes. But evolution did not stop there. The hooping increase in use of Smartphones and akin devices reflects the fast growth of urban and remote lifestyles. The Smartphone users are able to communicate worldwide within fraction of seconds. Number of successful business deals, transaction of money, goods and services are possible within no time; thanks to Smart technologies. Such technologies that have not only enabled text messages, but also audio and video calls over the same device with minimal infrastructure requirements are popularly known as Over-The-Top (OTT) applications. The worldwide use of such applications has certainly helped them bloom over a short time period. However, IT has not only helped people communicate at ease, but also, has opened avenues for miscreants to sniff communications by unauthorized means. Thus, insecurities and threats have crept in through the doors of convenience opened by OTT and other web applications for the users.

OTT and web applications were developed solely to facilitate communication amidst users. Preliminary applications never envisaged the vulnerabilities. Lately, such applications have been flooding the IT market. In order to win in this fierce battle of survival, these applications tend to address the Quality of Service (QoS) aspect alone, neglecting security aspects. Apparently, generic users seek high QoS, low latency in communication, high speed and high throughput in the shortest possible time. The application meeting all these criteria turns out to be clear winner and emerges popular worldwide. Such features are practically feasible with the classic trade-off concept amidst QoS and security. The higher the security, lower is the accuracy and QoS. Hence, developers have been compromising security aspect in order to thrive in IT business.

However, security and privacy became widely pronounced with IT hackers and cyber attackers vandalizing IT sector to greater extent. The cybercrimes in OTT and web applications like sniffing, tampering data, data theft, user security and privacy exploitation have become everyday news. Such incidents have curbed the use of these applications thereby affecting the IT market.

There have been scenarios where furious users have uninstalled applications and abandoned their use post security awareness. Such actions have brought in a major setback to the OTT and web applications domain. In order to meet the new security demands of the users, it has become important for the developers to cater to the security attributes of the applications. This paper highlights certain critical vulnerabilities and gaping holes of a very popular OTT and web application – WhatsApp. WhatsApp has been a common word in every household. From toddlers to old age group, WhatsApp has received a warm welcome. With every inching achievement and QoS rendered, it seems to be replacing much of the existing web applications like FaceBook Messenger and Skype

(Moore, 2016). As the concept of trade-off works amidst convenience and security, WhatsApp also falters in many places pertaining to security aspects.
In "Related Work" section, the paper will highlight existing work in the field of security pertaining to WhatsApp. "WhatsApp: Issues and Fixes" section will chronologically summarise the identified vulnerabilities in WhatsApp. "WhatsApp and Poor Authentication Technique" section will unravel a common yet unattended security issue encountered in WhatsApp and describe its impact on the users. In "Proposed Authentication Technique" section, we propose a novel solution to mitigate the issue and finally conclude in "Conclusion" section.

Related Work

WhatsApp and akin OTT and web applications have been a subject of interest for many researchers. What seems to be supporting our daily communication needs stays as a black box to us. Hence, researchers delve deep into the applications' architecture and skim the related threats and exploitation means. This section briefs the work of some researchers over the time pertaining to WhatsApp and similar applications.
In (Mueller et al., 2014), the authors report potential vulnerabilities of various OTT and web applications including WhatsApp that are vulnerable to enumeration issue owing to Phone Book access feature. In (Schrittwieser, et al., 2012), the authors explain the mechanism of exploiting verification mechanism of WhatsApp using SSL proxy. The authors also discuss other potential vulnerabilities associated with WhatsApp viz., Sender ID Spoofing, enumeration and unauthorized SMSes. In (Church & Oliveira, 2013), the authors distinguish the features of SMS application and WhatsApp application on the basis of users' survey. According to the survey, generic SMS feature of the Phones is considered safer in perspective of user's privacy than that of WhatsApp. The features of "Last Seen" and "2 Ticks" on the read messages, invade users' privacy. The features are not customizable by users thereby having no specific vantage for user's privacy. The participants of the survey mentioned certain other security and privacy issues associated with WhatsApp such as unencrypted WiFi access that could lead to interception of signals and security flaw wherein which people could send messages to devices without prior communication invitation. In (Kurowski, 2014), the author explains an attack to retrieve private information of WhatsApp user using the cell number information leaked by the application. The paper highlights the inflexible privacy settings of WhatsApp that could be exploited to seek information of a user. In (Cohn-Gordon et al., 2017), the authors conduct a forensic analysis of the Key Agreement and Management Scheme of WhatsApp and other such applications.
The authors also recommend potential modifications to ensure robustness of the scheme. Naiakshina et al., 2016, conducted a survey of students to perceive the security of WhatsApp and similar applications and discuss certain recommendations provided by the users. Ferreira et al., 2015, conducted experiments and surveys to analyse users' perspective w.r.t. security and privacy in such applications. It is inferred that, users are not comfortable sharing their phone book with the application.

WhatsApp: Issues and Fixes

WhatsApp has evolved as the most popular application that is gradually replacing Facebook Messenger and Skype with its advanced features. Notwithstanding, this application had major flaws that were fixed over time. Some of them are listed in Table 1.

WhatsApp and Poor Authentication Technique

There have been major concerns raised over the time pertaining to the application and most of them have been fixed. However, there exists a common problem that still remains unattended. Since Smartphones have become lightweight, more convenient for portability and easily accessible, it is inevitable that, they can be carried, stealthily picked, confiscated and stolen easily. This gives enough scope for hackers and honest-but-curious people to explore the contents of Smartphone of the actual users. Imagine a daily life scenario, where Eve could access Smartphone of Alice without her knowledge or in her absence. The curious mind of Eve provokes to sniff Alice's WhatsApp messages or have Command and Control (C&C) over her WhatsApp account. This will be possible only if Eve successfully logs into Alice's account. Shockingly, such remote access and control of WhatsApp is possible due to its weak authentication features. WhatsApp developers have leveraged the security levels with encryption techniques but have not been equally concerned about the authentication features. This section describes the issue in detail along with the relevant vulnerabilities.
In the present version, WhatsApp allows its user to access his/ her account on other devices with the help of the registered contact number alone. An OTP/ OTP on Call is forwarded to this registered contact number for verification. This feature can be misutilised by Eve in the aforementioned case study. It is assumed that Alice's phone does not have any security locking mechanism for incoming calls.

Year	Security Flaw
2011 (McCarty, 2011)	• "WhatsappHack" by GeenStijl – Flaw in authentication process. • WhatsApp application verified device, sent acknowledgement and the number from which message was sent; despite non receipt of verification request from the client. • Port 443 could be accessed and verification information was available to hacker that led to compromise of WhatsApp account of actual user.
2011 (Brookehoven, 2011)	• Poor implementation of SSL. • Allowed users on same network to read username, messages and phone numbers by mere use of WireShark. • Data intercepted in plain form as the messages do not traverse the channel in encrypted form.
2012(Kennell, 2012), (Morgan, 2012)	• WhatsApp account and associated data could be sniffed over public WiFi Network using WhatsApp sniffer. • Reverse engineering determines poor authentication i.e. uses MD5 Hash of reversed IMEI number for password verification purpose.
2012(Schellevis, 2012)	• Status of WhatsApp user's account could be changed arbitrarily.
2014(Khandelwal, 2014)	• Indrajeet Bhuyan and Saurav Kar find WhatsApp message handling technique vulnerable. Vulnerability gives scope to crash any WhatsApp account remotely.
2015 (Bhuyan, 2015)	• Privacy issue discovered by Bhuyan. • Users' privacy compromised via "WhatsApp Web Photo Sync Bug" and "WhatsApp Photo Privacy Bug" of "WhatsApp Web Client".
2017 (Ganguly, 2017)	• Encryption policy issue discovered by Tobias Boelter. • WhatsApp policy forces re-encryption of messages that are not delivered, without prior information to its recipients.

Table 1. Security Flaws in WhatsApp

This can give unauthorized access to the OTP on Call feature of WhatsApp. Hence, it is possible that Eve can first install WhatsApp on her own phone with the contact number of Alice. By misutilising the OTP on Call feature of WhatsApp, Eve can replicate Alice's WhatsApp account on her own phone. Additionally, by exploiting the vulnerability of WhatsApp discovered in 2017 (Ganguly, 2017), Eve can gain access to the old messages and data of Alice and thereby take C&C of Alice's WhatsApp account. Thus, such a simple form of attack is possible in an instant despite the default locking features of Smartphones.

Apart from the basic scenario, it is absolutely possible for any dedicated hacker to have C&C over a user's WhatsApp account. In this scenario, the hacker can exploit the SS7 vulnerability and register his/ her device with victim's phone number without getting physical access to victim's device. Hacker can redirect victim's call to his/ her mobile number or conduct an attack on SS7 network to get subscriber data such as International Mobile Subscriber Identity (IMSI). The hacker can trick a home subscriber network thereafter and register the victim in a fake roaming network. Finally, the hacker can receive all calls and text messages of the victim and gain access to his/ her WhatsApp account.

It is also noted that, WhatsApp provides a feature for privacy using PASSCODE that is completely based on numeric values alone. This renders the entropy and key space of PASSCODE weak. Along with, there exists no limited attempts of device registration in WhatsApp. Combining the weakness of both these features, it is evident that, cracking the PASSCODE will be an easy task and thereby help in hacking WhatsApp account. The advanced feature of WhatsApp also includes disabling the account in compromised phone. However, this technique is a curative measure and completely relies on victim's ability to timely access the phone and thereby determine the invasive action.

Proposed Authentication Technique

We infer that, the loopholes of registration and authentication mechanism of WhatsApp are trivial but can have adverse impact on the security of user's account. Hence, we propose certain features and security policies that can enhance the registration and authentication mechanism. This involves modification of the security architecture of the application such as introduction of security questions

that can replace the PASSCODE feature. Further, attempts of device registration should be limited to prevent any kind of brute force and Denial of Service (DoS) attacks. The proposal of modified architectural overlay to enhance the security features of WhatsApp is detailed in this section. The security architecture is modified for three different scenarios of registering and accessing WhatsApp application:-

1. First time registration by a new user using his/ her contact number.
2. Second time registration on a different device using existing contact number.
3. Maximum number of registration attempts on different devices for particular contact details.

First Time Registration by a New User using His/ Her Contact Number

During the first time registration, the proposed architecture will ask the user for his/ her contact number and email address. Post entry, the user will be prompted to select at least three user specific security questions and set answers for them.

The answers to the set questions will be sought only during re-registration process. Hidden input field will be provided for typing answers to prevent visual hacking in either case of registration or re-registration. Post setting of security questions and answers, the registration notification and OTP will be forwarded to registered contact number of the user. After providing the right OTP, a confirmation link regarding device access notification will be forwarded to the registered E-Mail address of the user. If the confirmation of the link is successful, then WhatsApp is registered successfully for the contact number, else registration fails. WhatsApp server will send an SMS on the registered contact number stating the successful registration of WhatsApp along with details of registration such as E-Mail address and contact number. This SMS will be sent randomly at any time within 48 hours of registration process. The proposal intends to solve two adversarial scenarios. We assume that, in both the cases, the adversary has temporary access to victim's device. Firstly, the adversary has partial knowledge of victim's credentials i.e. knowledge of contact number alone. In such a scenario, the adversary trying to misutilise the contact number will be blocked out of subsequent steps of registration due to lack of knowledge of victim's E-Mail credentials. Secondly, the adversary has full knowledge of victim's credentials or uses his/ her E-Mail address instead of the victim's. Inevitably, in such a case, WhatsApp will get registered with victim's contact number, but the proposal provides scope of security alert to the victim via random SMS notification as discussed earlier. This method is first of its own kind intending to prompt the victim to report the anomaly and thereby secure his/ her credentials from misutilization. The entire procedure has been outlined in Figure 1.

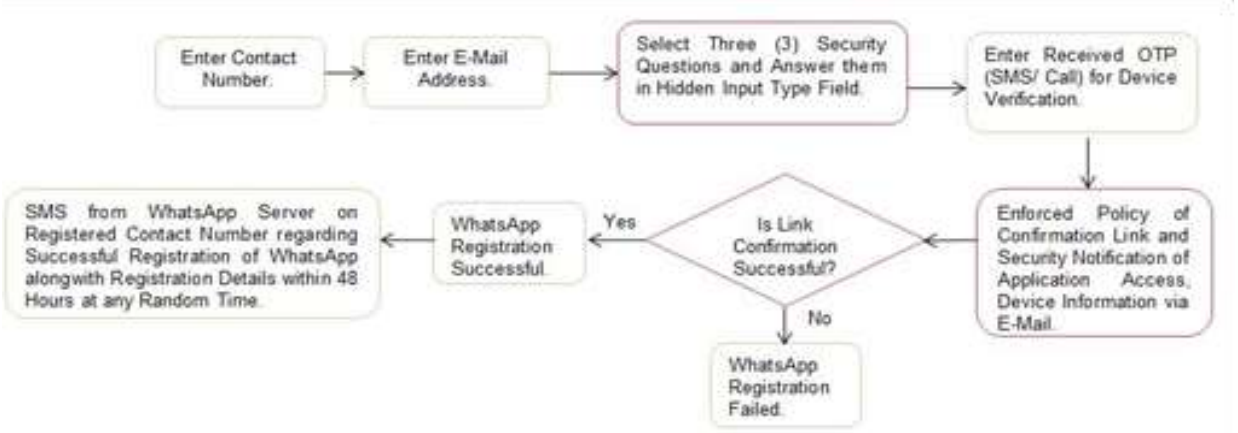

Figure 1 First Time Registration on WhatsApp using New Contact Details

Second Time Registration on a Different Device using Existing Contact Number

During the second time registration, the proposed architecture will ask the user for his/ her existing contact number and E-Mail address. An OTP will be generated and sent to user's number. The user will be asked to provide the OTP for verification. Post entry, one question out of the three user specific security questions (see "First Time Registration by a New User using His/ Her Contact Number" subsection) will pop randomly and seek user's answer. The answer will be typed in the hidden input field to prevent visual hacking. On correct entry, a link based re-registration notification and details of the device accessed will be sent to user's E-Mail address. On successful accessibility to the link, the re-registration process will

be rendered successful or else, the procedure will fail. This technique is advantageous owing to the fact that, despite the knowledge of OTP, a malicious user will not be able to access the account of genuine user. In order to access the account, the malicious user must have a prior knowledge of registered E-Mail address and password. Furthermore, the steps of access in the proposal is aligned strategically such that, knowledge of one-step alone does not grant re-registration privilege to a user. For instance, a malicious user is aware of the OTP via SS7 flaw. Yet, he/ she must know the answer to the security question following which he/ she must have access to E-Mail account of the genuine user. Furthermore, the security question is asked post OTP verification and not the other way round. This is because, security questions are not time bounded unlike OTP. In later case, there exists possibility of retrieving security answer via social engineering and then providing OTP for verification, thereby clearing two obstacles. But in proposed mechanism the attack method will be highly infeasible.

Maximum Number of Registration Attempts on Different Devices for Particular Contact Details

In the current architecture, there exists no limit on number of devices to be registered for an already registered contact number. With the scope of security questions alone, a hacker can exhaustively attempt security question's answer until attaining success. The new proposed architecture will therefore, equip a policy such that maximum number of registered devices for a unique mobile number should not exceed by 40. We have taken 40 as the number, w.r.t. to the survey (Victor, 2011). Figure 2 outlines the re-registration procedure along with solution for registration attempts.

Conclusion

It is inferred that, a secure and robust registration and authentication architecture of WhatsApp and similar web applications can curb the potential threats to a major level. As we observed, a minimalistic hacking attempt is possible owing to OTP on Call feature, it is concluded that, the proposed security architecture can bring in a revolution in the security protocol of the application. The intricate steps of confirmation involved are onetime activities. Hence, it is concluded that, these extensive steps will not hamper the regular use of the application once it has been genuinely registered. Furthermore, it is highlighted in (McCarty, 2011), how a hijacked WhatsApp user remains unaware of the account signup on other device.

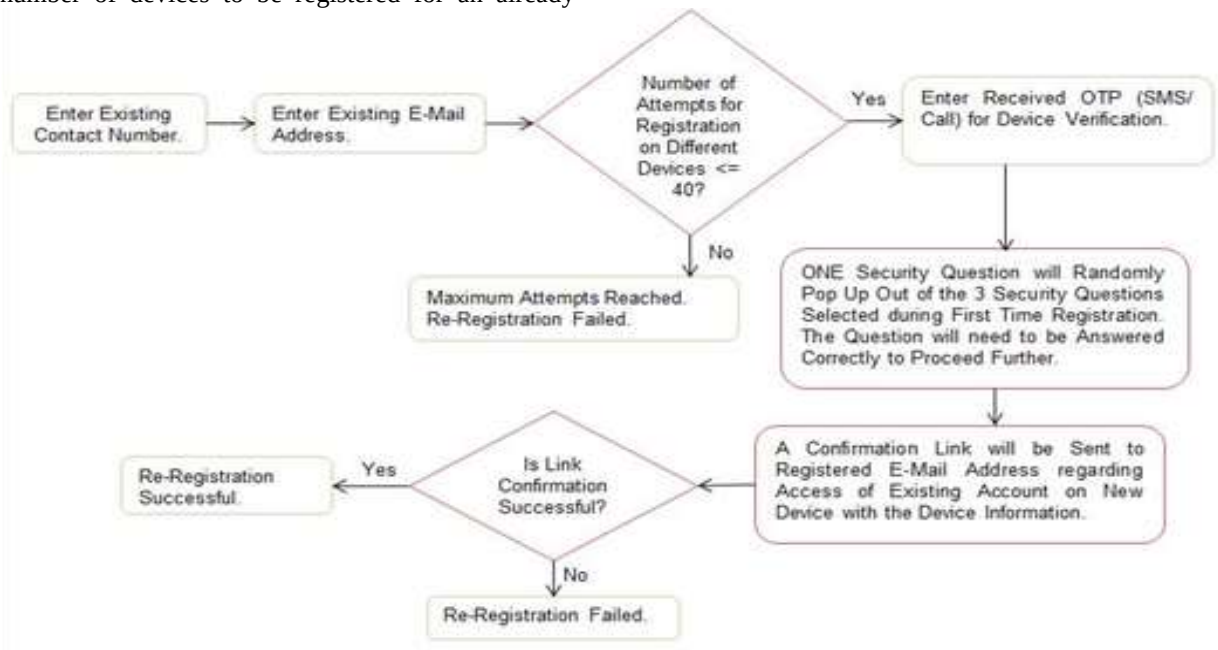

Figure 2 WhatsApp Re-registration with Existing Contact Details on Different Device

With our proposed solution pertaining to re-registration procedure, it is evident that the observed security flaw as mentioned in (McCarty, 2011) can also be mitigated. The paper highlights a proposal that has potential to curb adversarial scenario. In future we intend to simulate our case study, bring up experimental evidences, enhance the proposed security architecture with device information and induce identity based encryption. We also intend to build such a model in similar OTT and web

applications and analyse the security impact it has against hacking and C&C of user accounts.

References

1. Bhuyan, I. (2015, February). Multiple Vulnerabilities Found In Whatsapp Web. Retrieved January 21, 2018, from www.hackatrick.com: http://www.hackatrick.com/2015/02/multiple-vulnerabilities-found-in.html

2. Brookehoven, C. (2011, May 19). WhatsApp leaks usernames, telephone numbers and messages. Retrieved January 21, 2018, from www.yourdailymac.net: https://web.archive.org/web/20110523235136/http://www.yourdailymac.net/2011/05/whatsapp-leaks-usernames-telephone-numbers-and-messages/

3. Church, K., & Oliveira, R. d. (2013). What's up with whatsapp?: comparing mobile instant messaging behaviors with traditional SMS. 15th international conference on Human-computer interaction with mobile devices and services (MobileHCI '13) (pp. 352-361). New York, NY, USA: ACM.

4. Cohn-Gordon, K., Cremers, C., Dowling, B., Garratt, L., & Stebila, D. (2017). A Formal Security Analysis of the Signal Messaging Protocol. {IEEE} European Symposium on Security and Privacy, EuroS&P (pp. 451-466). Paris, France: IEEE.

5. Ferreira, D., Kostakos, V., Beresford, A. R., Lindqvist, J., & Dey , A. K. (2015). Securacy: an empirical investigation of Android applications' network usage, privacy and security. 8th ACM Conference on Security & Privacy in Wireless and Mobile Networks (pp. 1-11). New York: ACM.

6. Ganguly, M. (2017, January 13). WhatsApp design feature means some encrypted messages could be read by third party. Retrieved January 21, 2018, from https://www.theguardian.com/: https://www.theguardian.com/technology/2017/jan/13/whatsapp-design-feature-encrypted-messages

7. Kennell, K. (2012, September 12). WhatsApp is broken, really broken. Retrieved January 21, 2018, from fileperms.org: https://web.archive.org/web/20150108072201/http://fileperms.org/whatsapp-is-broken-really-broken.html

8. Khandelwal, S. (2014, December 01). Crash Your Friends' WhatsApp Remotely with Just a Message. Retrieved January 21, 2018, from https://thehackernews.com/2014/12/crash-your-friends-whatsapp-remotely_1.html

9. Kurowski, S. (2014). Using a whatsapp vulnerability for profiling individuals. Open Identity Summit, (pp. 140-146). Stuttgart, Germany.

10. McCarty, B. (2011, May 24). Signup goof leaves WhatsApp users open to account hijacking. Retrieved January 21, 2018, from www.thenextweb.com: https://thenextweb.com/apps/2011/05/23/signup-goof-leaves-whatsapp-users-open-to-account-hijacking/

11. Moore, M. (2016, November 15). WhatsApp just gave you a reason to uninstall Skype and Facebook Messenger. Retrieved January 21, 2018, from Express: https://www.express.co.uk/life-style/science-technology/732380/whatsapp-video-calls-official-windows-ios-windows-phone-app-update

12. Morgan, D. W. (2012, May 13). Sniffer tool displays other people's WhatsApp messages. Retrieved January 21, 2018, from The H Security: http://www.h-online.com/security/news/item/Sniffer-tool-displays-other-people-s-WhatsApp-messages-1574382.html

13. Mueller, R., Schrittwieser, S., Fruehwirt, P., Kieseberg, P., & Weippl, E. (2014). What's new with WhatsApp and Co.? Revisiting the security of Smart phone messaging applications.16th International Conference on Information Integration and Web-based Applications & Services (iiWAS '14) (pp. 142-151). New York, NY, USA: Maria Indrawan-Santiago, Matthias Steinbauer, Hong-Quang Nguyen, A. Min Tjoa, Ismail Khalil, and Gabriele Anderst-Kotsis (Eds.). ACM.

14.Naiakshina, A., Danilova, A., Dechand, S., Krol, K., Sasse, M. A., & Smith, M. (2016). Poster: Mental Models – User understanding of messaging and encryption. European Symposium on Security and Privacy.

15.Schellevis, J. (2012, January 12). WhatsApp status of others can still be changed. Retrieved January 21, 2018, from https://tweakers.net/: https://tweakers.net/nieuws/79321/whatsapp-status-van-anderen-is-nog-steeds-te-wijzigen.html

16. Schrittwieser, S., Frühwirt, P., Kieseberg, P., Leithner, M., Mulazzani, M., Huber, M., et al. (2012). Guess Who's Texting You? Evaluating the Security of Smartphone Messaging Applications. NDSS. The Internet Society.

17. Victor, H. (2011, June 11). Americans replace their cell phones every 2 years, Finns – every six, a study claims. Retrieved January 21, 2018, from https://www.phonearena.com/: https://www.phonearena.com/news/Americans-replace-their-cell-phones-every-2-years-Finns--every-six-a-study-claims_id20255

